ARTÍCULO DOI 10.52781/cmm.a082

Amenazas al Ciberespacio, Logística y Seguridad Nacional No necesariamente en ese orden

Cyberspace, Logistics and National Security Threats, not Necessarily in that Order

Resumen: ¿Cuál es la relación entre las vulnerabilidades cibernéticas, la logística y la seguridad nacional? Preocupaciones sobre la posible explotación de las vulnerabilidades del ciberespacio para causar ineficiencia logística en asuntos de seguridad nacional han persistido durante casi un cuarto de siglo. Este artículo actualiza el panorama de este debate y amplía el análisis a las amenazas recíprocas que plantean estas tres áreas. Se utiliza una metodología descriptiva, basada en estudios de casos de fuentes gubernamentales, artículos académicos y artículos periodísticos, para correlacionar el ciberespacio, las cadenas logísticas y la seguridad nacional. Se muestra que, además del sentido común de que los ciberataques pueden explotar vulnerabilidades existentes en diferentes niveles de la creciente automatización presente en los sistemas logísticos, presentando nuevas amenazas que pueden inhabilitar sistemas militares o infraestructuras civiles relevantes para la seguridad nacional, existe una amenaza creciente planteada por la complejidad logística a los productos cibernéticos y a la seguridad nacional, así como una 'armamentización' (*weaponisation*) de las decisiones de seguridad nacional de algunos países que ponen en peligro las cadenas de suministro, cibernéticas o no, de otras naciones con repercusiones en el desarrollo de sus capacidades de defensa.

Palabras clave: ciberespacio; gestión de las cadenas de suministro; gestión estratégica.

Abstract: What is the relationship between cyber vulnerabilities, logistics and national security? Concerns about the potential exploitation of cyberspace vulnerabilities to cause logistical inefficiency in national security matters have lingered for nearly a quarter of a century. This article updates the landscape of this debate and extends the analysis to the reciprocal threats posed by these three areas. A descriptive methodology, based on case studies obtained from government sources, academic articles and news articles, is used to correlate cyberspace, logistics chains and national security threats. It is demonstrated that, in addition to common sense that the exploitation of existing cyber vulnerabilities at different levels of the increasing automation present in logistical systems presenting new threats that can disable military systems or civil infrastructures relevant to national security, there is a growing threat posed by the logistical complexity to cybernetic products and national security, as well as a 'weaponisation' of national security decisions of some countries that jeopardize supply chains, cybernetic or not, of other nations, with reflexes in the development of their defence capabilities.

Keywords: cyberspace; supply-chain management; strategic management.

Marcelo Malagutti
Instituto Vegetius.
Brasília, DF, Brasil.
marcelo.malagutti@vegetius.org.br

Recibido: 22 oct. 2021
Aprobado: 25 jul. 2022

COLEÇÃO MEIRA MATTOS
ISSN on-line 2316-4891 / ISSN print 2316-4833
http://ebrevistas.eb.mil.br/index.php/RMM/index

1 Introducción

Ya es de sentido común que explotar las vulnerabilidades cibernéticas puede desactivar o dañar gravemente los sistemas logísticos críticos y, por lo tanto, comprometer la seguridad nacional. Sin embargo, ¿sería este el único orden de causalidad entre estas variables? Este artículo argumenta que no lo es. Como se demostrará, las evidencias empíricas confirman que las cadenas de suministro pueden utilizarse para comprometer las capacidades cibernéticas y afectar la seguridad nacional. De manera similar, se muestra que las decisiones de seguridad nacional de un país afectan las cadenas logísticas que crean vulnerabilidades cibernéticas. Por lo tanto, bajo ciertas condiciones, los tres factores pueden relacionarse causalmente en cualquier orden.

Para ello, se utilizó un método de investigación descriptivo del tipo *associations'* (GERRING, 2012). El método se aplica usando la lente del pensamiento de los Estudios Estratégicos, buscando patrones recurrentes de fuerza efectiva (no necesariamente militar) para vencer voluntades opuestas en situaciones de conflicto. Este enfoque impregna las obras de Clausewitz (1976), Liddell Hart (1930, 1931), Aron (2002), Beaufre (1965), Howard (1979), Freedman (1998, 2015), Gray (2008) y Stone (2007), para nombrar unos pocos. La selección de casos y documentos de referencia abarcó los últimos 10 años, con la notable excepción del Destinatario Elegible, utilizado como guía del problema idealizado.

El documento está estructurado de la siguiente manera. Después de esta introducción, una segunda sección presenta una breve introducción a la logística, mientras que una tercera describe brevemente su encuentro con el ciberespacio. Una cuarta sección presenta dos ejemplos clásicos de ciberataques que comprometieron los sistemas de defensa, mostrando el tradicional orden de causalidad entre las tres variables analizadas. Un quinto apartado ejemplifica los riesgos de incapacitación logística de las fuerzas militares en el teatro de operaciones, tanto desde el punto de vista del abastecimiento como de la comunicación y el control, ejemplificando el caso de los ciberataques que amenazan la logística y la seguridad nacional. Una sexta sección presenta las amenazas que plantean los procesos de fabricación de software y hardware, con una cadena de suministro compuesta por múltiples puntos de contacto explotables para implementar vulnerabilidades. Esta situación apunta a la logística que amenaza la seguridad cibernética y la seguridad nacional, con una subsección que analiza los esfuerzos de los gobiernos para enfrentarlos. Una séptima sección analiza la "armamentización" de la cadena de suministro cibernética, cuyas decisiones de seguridad nacional amenazan la logística de los productos cibernéticos. Finalmente, se hacen breves consideraciones sobre las conclusiones de este trabajo.

2 Una (muy) breve introducción a la logística

Una definición bien aceptada de logística empresarial la presenta como "el proceso de planificar, implementar y controlar el flujo y el almacenamiento eficientes y efectivos de bienes, servicios e información relacionada desde el punto de origen hasta el punto de consumo con el fin de cumplir con requerimientos del cliente" (WOOD, 1998).

El estudio de la Logística como ciencia se originó en las fuerzas armadas. Vegécio, en el siglo IV o V, ya dedicaba una parte importante de su obra a los fundamentos del abastecimiento militar (VEGETIUS, 1767). Sin embargo, el término en sí deriva del *Mayor General de Logis*, un militar cuya función "antes era albergar y acampar las tropas, dar dirección a las marchas de las columnas y ubicarlas sobre el terreno" (JOMINI, 1862, p. 188). A lo largo de los años, este conjunto básico de funciones se ha ampliado con la creciente complejidad de los ejércitos y las batallas. Curiosamente, Clausewitz, a menudo considerado el teórico de la guerra occidental más influyente, no dio una definición de logística ni usó un término específico para describirla. Esto lleva a los académicos a argumentar que consideraba "todo lo necesario para que la fuerza de combate se dé por supuesta" (PROENÇA JÚNIOR, DUARTE, p. 645).

Actualmente, en las ciencias militares, Logística se refiere a "todas las actividades de las unidades de las fuerzas armadas en apoyo de las unidades de combate, incluyendo transporte, abastecimiento, comunicación de señales, asistencia médica y similares" (LEIGHTON, 2022). La dificultad de encontrar un término específico que pueda, sin prejuicios, englobar y definir con precisión esta elaborada lista de actividades aún persiste en la actualidad (LEIGHTON, 2022). La importancia de la logística para los militares se expresa, de hecho, en la cita "los aficionados hablan de tácticas, pero los profesionales hablan de logística", "atribuida a todos, desde Napoleón Bonaparte hasta Omar Bradley" (EPSHTEIN; FAINT, 2019).

Las cadenas de suministro son los flujos de bienes e información dentro y entre organizaciones, "vinculados por una serie de habilitadores tangibles e intangibles, que incluyen relaciones, procesos, actividades y sistemas de información integrados" (PECK, 2012, p. 196). Son "el mecanismo en el corazón de la globalización de las últimas décadas mediante el cual las materias primas, las piezas y los componentes se intercambian a través de múltiples fronteras nacionales antes de incorporarse a los productos terminados" (SUPPLY..., 2019).

La adquisición, almacenamiento y distribución de cientos de miles de elementos de municiones, armamento, vehículos (con sus correspondientes repuestos y servicios de mantenimiento), combustible, uniformes, alojamiento, alimentación, salud e higiene, con complejas cadenas de suministro, que deben operar en terrenos difíciles, con medios de transporte restringidos y en condiciones de combate, es una tarea de enorme complejidad.

El combustible y los armamentos deben almacenarse en una zona de combate con munición suficiente para su defensa. De lo contrario, el enemigo podría apoderarse de estos arsenales de combustible y armas, con un doble impacto negativo: perderlos y usarlos contra sus dueños originales. Por lo tanto, es fundamental contar con la cantidad necesaria y suficiente de cada elemento de suministro en cada área de actividad. Los mismos principios se aplican a la logística civil: las corporaciones buscan eliminar inventarios innecesarios con el mismo esfuerzo que tratan de evitar la indisponibilidad de ítems que puedan comprometer sus operaciones.

A pesar de operar en diferentes escenarios, las cadenas logísticas militares y civiles persiguen los mismos objetivos principales. El foco ya no es *orientado a la masa* , pero *orientado a la velocidad*, con apenas inventarios necesarios y suficientes, distribución confiable, costos adecuados, cadenas de suministro confiables y entrega *just-in-time* o *bajo demanda* (KRESS, 2002).

3 En qué punto se encuentran la logística y el ciberespacio

La efectividad, la combinación resultante de eficiencia (hacer algo correctamente) y eficacia (hacer lo que hay que hacer), es un imperativo para la logística. Como tal, la automatización se ha asociado históricamente con la gestión de la cadena de suministro.

La logística moderna requiere información dinámica sobre toda la cadena de suministro, llamada 'In-Transit View' (KRESS, 2002). Dichos controles están fuertemente soportados por sistemas informáticos, cualquiera que sea la forma de contratación, control de costes, inventario o distribución que se adopte. Los datos generados en puntos dispersos, ya sean de solicitantes, proveedores o transportistas, se recopilan y procesan de forma integrada en tiempo real. El usuario informa su posición y necesidad; el sistema verifica la disponibilidad de los proveedores e informa el precio y la fecha estimada de llegada (ETA) al usuario, quien puede confirmar o no el pedido. Si se establece la aceptación, el usuario puede seguir el movimiento del artículo hacia él y la ETA ajustada en tiempo real.

Asimismo, los sistemas informáticos permiten medir la demanda, determinar la ubicación y el tamaño de los inventarios, demandar a los proveedores, en ocasiones incluso sin interacción humana, controlar y monitorear la distribución de los ítems, y también determinar el cambio en los planes operativos, proporcionando 'visibilidad completa de los activos' (KRESS, 2002).

Los vehículos autónomos, bien como la inteligencia artificial, "pueden cambiar fundamentalmente la forma en que operan las cadenas de suministro y cómo utilizan sus datos, sistemas y activos integrados"; estos nuevos niveles de automatización aumentarán la eficiencia y reducirán los costos operativos (TURNBULL, 2018, p.45). Como parte fundamental de lo que ahora se denomina Industria 4.0, se espera que la Fabricación Aditiva (impresión 3D) permita la producción local de repuestos y ítems bajo demanda, simplificando así las necesidades de transporte y almacenamiento y los riesgos asociados. En 2015, el Laboratorio de Investigación de Ingeniería de Construcción del Centro de Investigación y Desarrollo de Ingenieros del Ejército de EE. UU. estableció la Construcción Automatizada de Estructuras Expedicionarias (ACES). Su objetivo es desarrollar una tecnología de impresión 3D confiable y fácil de usar, capaz de generar estructuras militares expedicionarias personalizadas bajo demanda, en el campo, utilizando materiales disponibles localmente (JAGODA *et al.*, 2020, p. 2). En enero de 2021, el Departamento de Defensa de EE. UU. publicó su Estrategia de Fabricación Aditiva del Departamento de Defensa para alinear la impresión 3D con la misión del DoD (UNITED STATES, 2021a, p. 4). Los militares de EE. UU. ahora pueden "imprimir" piezas de repuesto para submarinos, Humvees e incluso bombarderos estratégicos B-52, y ha pedido una unidad de fabricación 3D portátil del tamaño de un contenedor que podría desplegarse en tierra y mar (BURTON; MCBIRNEY, 2022; SCHWAAR, 2022).

Sin embargo, a pesar de cuán vitales son las ventajas de una mayor automatización, también tienen desventajas relevantes. Con el impulso hacia la automatización, los sistemas logísticos estarán cada vez más conectados y segmentables (TURNBULL, 2018). No en vano, el informe del Departamento de Defensa de EE. UU. emitido en 2022, en atención a la Orden Ejecutiva de la Cadena de Suministro de América de 2021, hace 88 referencias a términos "cibernéticos", más de un tercio de las 251 referencias a "cadena de suministro" (BIDEN JR, 2022; UNITED STATES, 2022a).

Los avances tecnológicos plantean el espectro de una carrera armamentista en la seguridad de la cadena de suministro, con piratas informáticos privados y patrocinados por el Estado que tiene ventaja sobre las corporaciones y los gobiernos (SUPPLY..., 2019). Además, las cadenas de suministro ya son uno de los "tres principales vectores de ciberataques" (junto con las redes y personas internas) (NYE JR, 2017, p. 50). Por lo tanto, aún queda mucho por hacer para proteger las cadenas de suministro de ataques a través de dispositivos informáticos (LEE; MOLTKE, 2019).

4 Ciberamenazas a los Sistemas Logísticos de Seguridad Nacional

Esta sección presenta el caso clásico de amenazas cibernéticas que ponen en riesgo la logística relevante para la Seguridad Nacional.

Hace casi un cuarto de siglo, en junio de 1997, el Estado Mayor Conjunto de los Estados Unidos llevó a cabo un ejercicio llamado *Eligible Receiver* para probar las defensas cibernéticas estadounidenses. El escenario propuesto era el de una crisis que obligaría a Washington a enviar rápidamente tropas y aviones a Corea del Sur. Treinta y cinco expertos de la Agencia de Seguridad Nacional (NSA) conformaron el 'equipo rojo', simulando piratas informáticos al servicio de Corea del Norte con la misión de subvertir la operación estadounidense, utilizando únicamente equipos e información disponible públicamente. En apenas dos semanas, utilizando solo computadoras comerciales y programas de piratería descargados de Internet, este equipo rojo podría "piratear simultáneamente las redes eléctricas de nueve ciudades estadounidenses y romper sus sistemas de emergencia 911" (ADAMS, 2001, p. 101).

"Habiendo asegurado el caos civil y distraído a Washington", los hackers atacaron las redes informáticas del Pentágono, logrando "vagar libremente por las redes, sembrando destrucción y desconfianza por donde pasaban" (ADAMS, 2001, p. 101). Por ejemplo, dirigir los suministros a los destinos equivocados, lo que podría paralizar los aviones de combate de última generación debido a la falta de combustible, repuestos y armas (ADAMS, 2001).

Del mismo modo, la explotación de vulnerabilidades cibernéticas en la logística militar puede estar detrás de la desactivación de radares y baterías antiaéreas computarizadas, como probablemente hicieron los israelíes en la Operación Orchard antes de embarcarse en un ataque aéreo contra las supuestas instalaciones nucleares de Siria en Deir Ez-Zor (LIFF, 2012).

Actualmente, el Consejo de Ciencias de la Defensa de EE. UU. (DSB) considera que los impactos de un ataque cibernético contra las cadenas de suministro son potencialmente espectaculares. Cada vez que EE. UU. está en conflicto, debe esperar ataques cibernéticos con la intención de corromper sus cadenas de suministro, hacer que sus misiles y bombas no funcionen, o incluso usarlos contra las propias tropas estadounidenses. Los suministros, incluidos alimentos, agua, municiones y combustible, no podían llegar a donde ni cuando se necesitaban. Los comandantes militares perderían rápidamente la confianza en la información y la capacidad de controlar sus sistemas y fuerzas. Una vez perdida, la confianza es difícil de recuperar (UNITED STATES, 2013b).

En 2013/14, el Comité de Servicios Armados del Senado de EE. UU. investigó ciberataques que involucraron al Comando de Transporte del Departamento de Defensa (DoD) de EE. UU (TRANSCOM) y once de sus proveedores. El informe resultante señala que el comité se

centró en TRANSCOM debido a su papel central en las "operaciones de movilización, despliegue y sostenimiento y los recursos críticos que los contratistas de TRANSCOM proporcionan para cumplir con los requisitos militares en las operaciones de contingencia" (BRYAN *et al.*, 2014). El informe establece que las compañías aéreas privadas proporcionan más del noventa por ciento de la capacidad de manejo de pasajeros y más de un tercio de la capacidad bruta de manejo de carga DoD, mientras que el 95% de su carga seca es transportada por buques mercantes. Además, más del 90 % de las transacciones de despliegue y distribución del DoD se realizan en redes no clasificadas, muchas de las cuales son propiedad de empresas privadas, según una estimación del comandante de TRANSCOM (BRYAN *et al.*, 2014).

La investigación de TRANSCOM identificó 50 ciberataques o intrusiones realizadas entre el 1 de junio de 2012 y el 30 de mayo de 2013. Además, al menos 20 intrusiones exitosas en redes contratadas fueron clasificadas como Amenazas Persistentes Avanzadas (APT). El término se "utiliza para distinguir amenazas cibernéticas sofisticadas que a menudo se asocian con gobiernos extranjeros"; de estos, el comando fue informado de apenas dos, "un hallazgo preocupante dado el impacto potencial de las intrusiones cibernéticas en la información y las operaciones de defensa" (BRYAN *et al.*, 2014, p. i).

Entre las razones por las que TRANSCOM desconocía los ataques, se constató la existencia de vacíos en los requisitos contractuales de comunicación, además de la falta de entendimiento común entre el contratista y sus contratistas sobre el alcance de lo que se debe informar en relación con los ataques cibernéticos. Además, el Departamento Federal de Investigaciones (FBI) y el DoD a menudo no sabían que las empresas identificadas como víctimas de ataques cibernéticos eran proveedores de este comando (BRYAN *et al.*, 2014).

El Plan Estratégico 2015-2022 de la Agencia de Logística de Defensa de EE. UU. (DLA) estableció que la ciberseguridad constituye un riesgo operativo significativo que plantea desafíos severos para las cadenas de suministro de la DLA en todo los momentos. Por lo tanto, es necesario crear un entorno que fomente la denuncia y el combate a las ciberamenazas y que la misma atención se extienda a su base de proveedores, en que la DLA debe ser 'astuta' en la gestión de la relación para garantizar que los socios del sector privado protejan los suministros y la integridad los datos para brindar apoyo efectivo a los combatientes (UNITED STATES, 2015). La astucia intencionada puede reflejarse en el uso de PBL para "estimular" a los proveedores.

La investigación del Senado de EE. UU. encontró que todos APT identificados en TRANSCOM y sus proveedores se atribuyeron a China. También indicó que los analistas militares chinos han identificado la logística y la movilización como posibles vulnerabilidades de EE. UU. 'ofrecidos los requerimientos de precisión en las redes de coordinación, transporte, comunicación y logística' y que la doctrina militar china 'aboga aspirando al comando y control del adversario y logística redes para afectar su capacidad de operar durante las primeras etapas del conflicto'. Además, la investigación verificó que expertos estadounidenses en planificación militar china plantearon la posibilidad de que China pudiera usar capacidades cibernéticas para evitar el despliegue de fuerzas estadounidenses en caso de una contingencia (BRYAN *et al.*, 2014). Así, los chinos podrían buscar obtener, en un eventual conflicto con EE. UU. , las mismas ventajas que obtuvo el equipo rojo de la NSA en Eligible Receiver, hace 25 años.

Posiblemente, el efecto más relevante del Eligible Receiver fue el hecho de que los piratas informáticos también pudieron paralizar el sistema humano de Comando y Control (C2) con un alto nivel de desconfianza derivado de órdenes falsas de un comandante general, falsificando "noticias sobre el crisis e instrucciones de las autoridades civiles del comando" (ADAMS, 2001, p. 101).

> "Como resultado, nadie en la cadena de mando, desde el presidente en adelante, podía creer nada. Este grupo de piratas informáticos que utilizó recursos disponibles públicamente pudo evitar que Estados Unidos librara una guerra de manera efectiva" (ADAMS, 2001, p. 101).

C2 es también una función de logística militar. Si bien no es intrínsecamente una capacidad militar cibernética como muchas otras, se ha vuelto tan dependiente del ciberespacio que un oponente puede verse tentado a realizar un primer ataque cibernético paralizante contra ellos (MORGAN, 2010). Este proceso de degradación cibernético-C2, destinado a destruir (o al menos degradar en gran medida) la cohesión interna del oponente, podría potencialmente paralizar las fuerzas militares del enemigo objetivo y aumentar la eficacia de un ataque cinético posterior contra ellas.

Además, el armamento moderno ha dependido cada vez más de los circuitos integrados, y actualmente, la electrónica contiene un código programable de complejidad creciente. Al mismo tiempo, el DoD se ha convertido en un comprador mucho menos influyente en una amplia y globalizada base de proveedores. Por lo tanto, garantizar que los componentes electrónicos de defensa estén libres de vulnerabilidades es una tarea hercúlea (UNITED STATES, 2017).

Debido a que los ajustes de configuración en estos dispositivos permanecen sin cambios durante largos períodos, los componentes comprometidos pueden crear vulnerabilidades persistentes, y la explotación de estas vulnerabilidades en los componentes o en sus softwares integrados puede ocasionar fallas en el armamento moderno. Estas explotaciones son particularmente dañosas porque es difícil diferenciarlas de fallas eléctricas o mecánicas.

Además, un ciberataque en sí mismo no tiene por qué ser letal. Si degrada la eficacia de una fuerza militar o reduce la funcionalidad de las armas de precisión y los sistemas de selección de objetivos o la disponibilidad de combustible y suministros médicos, el resultado será mortal para la fuerza que depende de los recursos comprometidos (TURNBULL, 2018).

Sin embargo, dentro del ámbito de la Seguridad Nacional, además de las amenazas cibernéticas a la logística militar y C2, también existe la amenaza cibernética mencionada con frecuencia a la infraestructura civil crítica. Hasta hace poco, los casos más famosos fueron los relacionados con el suministro de energía de Ucrania en 2015, llamado Industroyer, y 2016, llamado CrashOverride, posiblemente lanzado por piratas informáticos rusos (AUCHARD; FINKLE, 2016; ZETTER, 2016). No obstante, en mayo de 2021, un ataque de ransomware atribuido a un grupo cibercriminal ruso llamado DarkSide golpeó el Oleoducto Colonial, dejando vastas partes de los EE. UU. con suministros restringidos de productos petrolíferos (SANGER; PERLROTH, 2021).

5 Amenazas logísticas a productos cibernéticos

Esta sección analiza el caso en el que la logística amenaza los productos cibernéticos y la Seguridad Nacional. Es de sentido común que un tornillo, fusible o componente químico adulterado en una cadena de suministro larga y difícil de controlar puede afectar el rendimiento o crear vulnerabilidades físicas en cualquier equipo militar. Sin embargo, un entendimiento menos notable es que, de manera similar, los componentes adulterados en la cadena de suministro extendida de productos de hardware o software pueden afectar el rendimiento o crear vulnerabilidades en ellos y en los sistemas que los utilizan. Para captar mejor este concepto, es necesario comprender la cadena de suministro de los productos cibernéticos, que el Instituto Nacional de Estándares y Tecnología de EE. UU. (NIST) denomina Cadena de Suministro Cibernética (NIST; FIREEYE, 2015).

Ya en 2001, oficiales de inteligencia estadounidenses creían "que ciertos equipos y software importados de Rusia, China, Israel, India y Francia" estaban infectados con "dispositivos" capaces de "leer datos y destruir sistemas", aunque esta sospecha fuera difícil de probar (ADAMS, 2001). Recientemente, se identificó hardware falsificado en sistemas adquiridos por el DoD (LYNN III, 2010). Como resultado, un informe de la Comisión Permanente de Inteligencia de la Cámara de EE. UU. en 2012 restringió la compra de equipos de las empresas chinas Huawei y ZTE (ROGERS; RUPPERSBERGER, 2012).

Los sistemas digitales de hoy en día son muy complejos, construidos por componentes de software y hardware superpuestos que están integrados en diferentes niveles y suministrados por múltiples proveedores de todo el mundo. La materialidad del hardware lo hace evidente, y es más probable que los humanos lo entiendan y lo acepten como riesgoso o inseguro. No obstante, el software es lo que 'anima' al hardware.

En el nivel de software muy básico, los dispositivos electrónicos a menudo son controlados por *firmware*, software grabado en sus componentes. Determina cómo funciona el equipo. Un ejemplo famoso es el Basic Input Output System (BIOS) de los procesadores, pero también existe en placas de circuito de red y video, escáneres o impresoras. Cada vez más, el hardware ofrece la posibilidad de actualizar su firmware, cambiando así el comportamiento operativo del dispositivo sin necesidad de reemplazarlo. El malware puede aprovechar las vulnerabilidades del firmware, por ejemplo, mediante la inserción de un kill switch que puede desactivar el hardware por orden del enemigo. Posiblemente peor, el malware puede hacer que los dispositivos se comporten de forma errática.

El firmware utiliza otra capa de software, la *driver*, para comunicarse con *Sistemas Operacionales* (SO) como Android, iOS, Windows o Linux. El mismo par de hardware y firmware (una impresora, por ejemplo) tiene diferentes controladores para comunicarse con diferentes SO. Un controlador adulterado puede modificar el funcionamiento de un dispositivo, engañando al SO. Este fue el principio detrás de Stuxnet, donde los Controladores Lógicos de Programación (PLCs) que conectan las centrífugas de enriquecimiento de uranio iraníes a su sistema de Supervisión de Control y Adquisición de Datos (SCADA) han sido reemplazados por otros mejorados. Entonces, si bien el sistema de control indicaba que las centrífugas estaban funcionando con regularidad, en realidad giraban fuera de ritmo y, por lo tanto, estaban físicamente dañadas (ZETTER, 2015a).

A un nivel superior, es posible contaminar el propio SO. En el caso de Snowden, se reveló que Cisco, el fabricante de activos de red más grande del mundo, tenía el SO de sus enrutadores y servidores (Cisco IOS) manipulado por la NSA (GREENWALD, 2014). En diciembre de 2015, Juniper Networks, el segundo mayor fabricante de activos de red, anunció el descubrimiento de un backdoor secreto en JunOS, el sistema operativo para sus firewalls. Se descubrió que se había ingresado en el código antes de 2011 (ZETTER, 2015b). No estaba claro quién habría desplegado este backdoor.

En agosto de 2016, Cisco anunció nuevamente el descubrimiento de una vulnerabilidad de día cero (de fábrica) en el Cisco IOS, implementada 13 años antes, que podría explotarse para garantizar el acceso total a las redes utilizando sus equipos. Se encontró al analizar el código del programa supuestamente perteneciente al Equation Group (hackers vinculados a la NSA) que fue 'filtrado' en Internet por el grupo de hackers Shadow Brokers (GOODIN, 2016). Por lo tanto, la NSA podría haber aprovechado esta vulnerabilidad para violar redes informáticas de interés estadounidense. Cisco encontró al menos otras ocho backdoors similares en su sistema operativo en 2017 y 2018 (CIMPANU, 2018; CISCO, 2017).

El siguiente nivel de software se llama *middleware*, el "software que se encuentra entre un sistema operativo y las aplicaciones que se ejecutan en él", "funciona esencialmente como una capa de traducción oculta" y permite la comunicación y la gestión de datos para las aplicaciones (MICROSOFT, 2022). Esta categoría incluye bases de datos y servidores web, entre otros. Las aplicaciones (Apps) se conectan a ellos a través de bibliotecas de software denominadas Interfaces de Programación de Aplicaciones (APIs) o Kits de Desarrollo de Software (SDKs). Estas APIs, que generalmente son desarrolladas por proveedores externos en diferentes partes del mundo, se pueden modificar en el proceso de incorporación.

Casi en la capa superior de software se encuentra el software Commercial-Off-The-Shelf (COTS), como plataformas de automatización de oficinas, sistemas de correo electrónico, generadores y lectores de PDF, y cientos de otros. Los archivos de documentos portátiles de Adobe (PDFs) blindados y los documentos de Microsoft Office han estado poniendo en peligro los sistemas durante algún tiempo (HUTCHINS; AMIN; CLOPPERT, 2010).

Finalmente, la capa de software superior son aplicaciones especializadas que ejecutan el "negocio principal" de las organizaciones, como los sistemas de logística. La complejidad de las aplicaciones modernas ha convertido el desarrollo de software en ensamblaje, en un contexto de desarrollo colaborativo, con componentes muy especializados (APIs) adquiridos a terceros, creando cadenas de suministro muy largas (SHERMAN, 2019).

La mayoría de estos componentes son *cajas negras*, con su código fuente invisible, aunque el software de Open-Source (OSS) está ganando terreno en la industria del software y aceptación en el ambiente militar (UNITED STATES, 2021b). La cadena de suministro de software se ha convertido en una red compleja de componentes dentro de los componentes de código descargados confiables de una organización que se utilizan para crear aplicaciones (BLESSMAN, 2019). Además, el software es "extremadamente maleable bajo la presión de la combinación correcta de toques con los dedos, lo que puede tener ventajas y debilidades estratégicas cuando se integra en el mundo a través de la confianza en la tecnología conectada" (WOODS; BOCHMAN, 2018).

En general, esta complejidad hace que sea crucial mantener estos diversos componentes actualizados, y es necesaria la administración continua de parches de software. La gestión de parches de software se complica por la fragilidad de los entornos de producción, en la que una multitud de aplicaciones y paquetes de soporte deben interactuar sin causar conflictos o fallas catastróficas (TURNBULL, 2018).

Además, una versión mejorada del software de una empresa contable ucraniana que contenía una carga útil destructiva llamada NotPetya paralizó las redes a nivel mundial, lo que les costó a los gigantes logísticos FedEx y Maersk más de US$ 300 millones cada uno (UNITED STATES, 2018). Se abusó de los mecanismos de actualización de software (¡de hecho, los sistemas de entrega!) para obtener acceso a los sistemas de control de la red (WOODS; BOCHMAN, 2018).

En otro caso famoso, en 2017, alrededor de 2,2 millones de clientes fueron infectados con un backdoor cuando los piratas informáticos, dirigidos a empresas como Samsung, Sony, Asus, Intel, VMWare, O2 y Fujitsu, secuestraron el sistema de actualización automática de CCleaner, un software antivirus y de seguridad (CORERA, 2018; UNITED STATES, 2018).

Recientemente, las investigaciones revelaron que SolarWinds, una empresa estadounidense que produce un software de administración de redes de TI llamado Orion, había sido infectada en octubre de 2019. El compromiso de esta cadena de suministro permitió el uso de la actualización de seguridad de software de rutina de Orion para instalar software malicioso en las redes de los clientes de SolarWinds. Este compromiso aseguró el acceso de los piratas informáticos a al menos nueve agencias federales de EE. UU. , incluidos el Departamento del Tesoro y el Departamento de Justicia, y "equipos de tecnología digital claves como Cisco, Intel, Nvidia y Microsoft, así como ciberseguridad empresas como FireEye" (WILLETT, 2021, p. 8).

La complejidad de la cadena de suministro de software desafía a la mayoría de los programas de seguridad empresarial, ya que los componentes modificados se vuelven difíciles de detectar y "las organizaciones simplemente confían en que sus proveedores están proporcionando software seguro, ofreciendo a los actores de amenazas una solución alternativa para vencer los procedimientos de seguridad de una organización" (BLESSMAN, 2019, p. 10).

Las vulnerabilidades en la cadena de suministro pueden introducirse o descubrirse a lo largo de todo el ciclo de vida de un producto de software, prestando especial atención al hecho de que la mayoría de los sistemas son desarrollados, adquiridos y distribuidos sin planes formales de protección (UNITED STATES, 2017).

5.1 Lidiando con la Cadena de Suministro Cibernética

La Estrategia para operar en el ciberespacio del DoD de 2011 presentó las vulnerabilidades y amenazas de la cadena de suministro a la capacidad operativa del DoD como uno de los "aspectos centrales de la ciberamenaza" (UNITED STATES, 2011). También establece que:

> Software y hardware corren el riesgo de sufrir una manipulación malintencionada incluso antes de que se integren en un sistema operativo. La mayoría de los productos de tecnología de la información que se usan en los Estados Unidos se fabrican y son ensamblados en el extranjero. La dependencia del DoD de la fabricación y el desarrollo en el extranjero crea desafíos en la gestión de riesgos en los puntos de diseño, fabricación, servicio, distribución y eliminación (UNITED STATES, 2011, p. 3).

Intuitivamente, uno podría verse intentado a proponer que el gobierno apruebe el hardware y el software extranjeros antes de que ingresen al mercado. En la práctica, sin embargo, esto no sería factible. El número de líneas de código fuente (SLOC) para productos de software comercial ha aumentado a aproximadamente cincuenta millones, y el gobierno de EE. UU. cree que este crecimiento continuará durante las próximas décadas (UNITED STATES, 2013b). Por el lado del hardware, los circuitos integrados complejos tienen hoy más de dos millones de transistores. Por lo tanto, es imposible probar completamente las fallas y vulnerabilidades de tales productos de software o hardware. Tratar de verificarlos en su totalidad llevaría años.

Estos productos complejos a menudo ingresan al mercado con bugs. Por ejemplo, en 1994, poco después de que los nuevos procesadores Pentium ingresaran al mercado, se reveló un error en su división de números de punto flotante, lo que la hizo bastante imprecisa (HALFHILL, 1995). Nuevamente, en 2020, se descubrió una nueva falla en todos los procesadores de la compañía producidos en los últimos cinco años que podría explotarse para obtener acceso a la seguridad del sistema (BLUMENTHAL, 2020).

En 2014, NIST publicó su Framework for Improving Critical Infrastructure Cybersecurity en una asociación entre el gobierno de EE. UU. y el sector privado, teniendo en cuenta que "al igual que el riesgo financiero y de reputación, el riesgo de seguridad cibernética afecta el resultado final de una empresa" (NIST, 2014). El principio central es que la ciberseguridad de la cadena de suministro no se trata solo de la tecnología de la información y la comunicación (TIC), sino que involucra a proveedores, distribuidores, gestión, continuidad y confiabilidad de la cadena de suministro, seguridad del transporte y otras actividades de seguridad.

Con base en su framework, el NIST comenzó a investigar no solo a las empresas de TIC, sino también a las empresas que utilizan ampliamente productos de TIC en sus procesos. Las empresas participantes incluyen Boeing, Cisco, Deere, Dupont, Fire Eye, Fujitsu, Intel, Juniper, Northrop Grumman, P&G y empresas de servicios públicos (o infraestructura). El objetivo era detectar cómo las empresas tratan temas como los siguientes (NIST, 2014):

- Proveedores externos con acceso físico o virtual a sistemas de información, códigos fuente de programas o equipos (desde limpieza hasta ingeniería de software);
- Prácticas inadecuadas de seguridad de la información por parte de sus proveedores;
- Productos de hardware o software comprometidos comprados a proveedores;

• Vulnerabilidades de seguridad de software en la gestión de la cadena de suministro o sistemas de proveedores;

• Hardware falsificado o malware integrado;

• Almacenamiento o agregación de datos por parte de terceros;

• Repetibilidad y trazabilidad del proceso de diseño y desarrollo de software o hardware;

• Capacidades del proveedor para resolver vulnerabilidades, incluidos 0 días.

Así, existe una creciente preocupación del gobierno estadounidense en cuanto a la garantía del Gestió de Riesgo de la Cadena de Suministros Cibernética (C-SCRM) con sus proveedores, y estos con los suyos, de forma recursiva (NIST; FIREEYE, 2015).

Cuando un gobierno compra productos o servicios con *fabricación* inadecuada o seguridad *integrada*, los riesgos persisten durante todo el ciclo de vida del ítem adquirido. Este efecto duradero forma parte de lo que hace el cambio en los procesos de adquisición sea tan importante para lograr la ciberseguridad y la resiliencia. La compra de productos y servicios con la seguridad de fábrica integrada adecuada puede tener costos iniciales más altos. Aún así, reduce el costo total de propiedad (TCO) debido a la mitigación de riesgos y a la reducción de la necesidad de corrección de vulnerabilidades en productos distribuidos o implementados en el campo (UNITED STATES, 2013a).

En los procesos de adquisición del DoD que suelen ser largos, alrededor del 70 % de los componentes electrónicos de los sistemas de armas están obsoletos o fuera de producción antes de que se implementen estos productos (UNITED STATES, 2017). Esto hace que se inserten nuevos componentes durante el proceso de producción, lo que dificulta aún más la validación de la integridad de estos componentes.

Como resultado, el malware se puede implementar en los sistemas informáticos (hardware + software) a medida que se desarrollan o construyen y se pueden usar para crear kill-switches y backdoors operados de forma remota, lo que permite a los atacantes manipular los sistemas en ejecución en situaciones de conflicto. Para contrarrestar este riesgo, las empresas privadas de software y hardware de los Estados Unidos se han asociado con el gobierno para crear mecanismos de seguridad. Por ejemplo, Microsoft y otras empresas informáticas desarrollan estrategias sofisticadas para detectar códigos maliciosos (como las backdoors de Juniper Networks y Cisco) y evitar su despliegue en sus cadenas de suministro globales (LYNN, 2010). A pesar de que en marzo de 2021, los piratas informáticos chinos utilizaron una falla en el producto del servidor de correo electrónico de Microsoft Exchange para obtener acceso a los datos y correos electrónicos de los usuarios, lo que afectó a "hasta 30.000 entidades públicas y privadas, principalmente pequeñas empresas y gobiernos locales" (WILLETT, 2021).

6 Armamentización De Seguridad Nacional De La Cadena De Suministro Cibernética

Finalmente, esta sección describe cómo las decisiones de Seguridad Nacional con respecto a las restricciones de exportación e importación arman las cadenas de suministro cibernéticas, lo que representa amenazas para la cadena de logística cibernética de otros países. Esto ejemplifica el tercer caso estudiado, en el que las decisiones de Seguridad Nacional afectan el ciberespacio y las cadenas logísticas en países extranjeros.

Desde 2015, el gobierno de EE. UU. ha prohibido que Intel revenda sus últimos procesadores a China, supuestamente porque se utilizarían para pruebas nucleares (CLARK, 2015). En 2018, el país recuperó las dos primeras posiciones en la lista de supercomputadoras, que anteriormente ocupaba China (TOP500.ORG, 2020). La diferencia entre los transformadores se refleja en los números presentados. Mientras que la estadounidense Sierra, en primer lugar, alcanza los 200 PFLOPS con 2,4 millones de núcleos y consume 10 MW de energía, la china TaihuLight, tercera en la lista, utilizando procesadores chinos, alcanza los 125 PFLOPS con 10,6 millones de núcleos y consume 15 MW (TOP500.ORG, 2020).

La solución china preferida, típica de cualquier país en desarrollo, es reemplazar las soluciones extranjeras por las nativas, una solución que requiere una fuerte capacidad de innovación y, contrariamente a la intuición, conexiones globales (LEWIS, 2018). China utiliza "campeones nacionales, los protege a nivel nacional y los ayuda a competir" a nivel mundial (LEWIS, 2018, p. 5-6). "[Si] China no hubiera bloqueado a Google, no habría Baidu" (LEWIS, 2018, p. 5-6). Sin embargo, "esta promoción de campeones nacionales por cualquier medio es la fuente de gran parte de las tensiones comerciales actuales, y los gobiernos occidentales están desarrollando lentamente respuestas que limitarán el crecimiento de China a menos que cambien sus políticas" (LEWIS, 2018, p. 5-6).

Hace más de 25 siglos, Sun Tzu escribió:

> Si conoces al enemigo y te conoces a ti mismo, no debes temer el resultado de cien batallas. Si te conoces a ti mismo, pero no al enemigo, por cada victoria que obtengas también sufrirás una derrota. Si no conoces ni al enemigo ni a ti mismo, sucumbirás en cada batalla (TZU, 2009, p. 13).

Tener informaciones de inteligencia forma parte del sentido común en la política. Además, las agencias de inteligencia siempre están buscando oportunidades para recopilar información confidencial a través de redes y dispositivos de TIC, incluso en tiempos de paz, y en relación con socios y aliados tradicionales. Ni siquiera los equipos suministrados por empresas de países tradicionalmente neutrales pueden considerarse insospechados e inalcanzables por sus tentáculos. Por ejemplo, la empresa suiza Crypto AG, fabricante de criptógrafos utilizados en más de 120 países, formó parte, entre 1970 y 2018, de una sociedad altamente sigilosa entre la CIA y el servicio de inteligencia alemán BND. El equipo de Crypto AG fue saboteado para que estas agencias pudieran acceder a la información cifrada en estos dispositivos (MILLER, 2020). En otro caso famoso, Snowden dejó claro que la NSA estaba espiando a decenas de aliados de Estados Unidos, incluidos Alemania, Brasil, Japón y México (GREENWALD, 2014).

Ahora, el gobierno de EE. UU. acusa a Huawei, el líder mundial en telefonía 5G, de tener vínculos turbios con la inteligencia china. Además, EE.UU. argumenta que prefiere el uso de equipos de la sueca Ericsson o de la finlandesa Nokia, aunque más caros, e personalidades del gobierno estadounidense han sugerido la adquisición de acciones para controlar estas empresas (KHARPAL, 2020).

Estados Unidos también está presionando a sus aliados para que veten el uso de la tecnología 5G china. En mayo de 2020, el Reino Unido anunció la prohibición de actuación de la empresa. Deutsche Telekom de Alemania (32% de propiedad estatal) respondió que excluir a Huawei de sus redes 5G sería un 'Armagedón' y, aunque no restringe su participación, anunció recientemente que se eligió a Ericsson (ALLEVEN, 2020; ERICSSON, 2020; PETZINGER, 2020). Bajo una enorme presión de EE. UU. por la participación de Huawei en las redes brasileñas, con el embajador de EE. UU. amenazando con 'consecuencias', los militares brasileños habrían dicho a su gobierno que "la misma exposición eventual que Brasil puede sufrir de la tecnología china con Huawei también ocurrirá con cualquier otra empresa" (AMADO *et al.*, 2020; ROSA; ANTUNES, 2020). De hecho, una posición muy pragmática, considerando los casos de Crypto AG, Cisco y Juniper, entre otros.

Del lado chino, en 2017, una nueva ley de ciberseguridad restringió la venta de tecnologías de información y comunicación extranjeras. Además, China ha exigido a las empresas extranjeras que presenten estos productos a las revisiones de Seguridad Nacional administradas por el gobierno y a las empresas que operan en China que almacenen sus datos en China, lo que requiere aprobación oficial antes de transferirlos a otros países (UNITED STATES, 2018). Como está claro que las revisiones de seguridad serán largas e imperfectas, esta parece ser una forma de poner barreras a la tecnología extranjera, un contraataque debido a las restricciones occidentales de Huawei.

Excluida del mercado estadounidense en 2019, Huawei respondió prohibiendo el uso de componentes estadounidenses. El gigante chino comenzó a trabajar para reemplazar estos componentes con versiones chinas (STRUMPF, 2020). Sin embargo, incluso esa estrategia se vio amenazada cuando el Departamento de Comercio de EE. UU. dio un paso adelante en mayo de 2020 y prohibió a los fabricantes de componentes que utilizan tecnología estadounidense en todo el mundo vender productos a Huawei (UNITED STATES, 2020). Esta nueva dificultad puede incluso sacar a la empresa de su posición dominante en la carrera del 5G y poner en peligro el mantenimiento de las redes telefónicas de otras generaciones proporcionadas por la empresa y ya en uso en varios países (STRUMPF, 2020). Además, EE. UU. está considerando ahora bloquear el suministro de tecnología estadounidense a cinco empresas chinas de videovigilancia (SHIDONG, 2019).

Las restricciones de uso no solo se refieren al hardware, sino también al software. El veto del gobierno de EE.UU. a Huawei impide a Google licenciar el uso del sistema operativo Android en los teléfonos de la compañía (MOON, 2019). Aunque el núcleo de Android es de código abierto, por lo que la empresa china puede seguir usándolo, varios servicios asociados son proporcionados por Google y ya no estarían disponibles, lo que limita la utilidad de los teléfonos inteligentes de Huawei (MOON, 2019).

En medio del embargo de EE. UU. sobre el suministro de tecnología a China, Beijing ordenó a todas las oficinas gubernamentales e instituciones públicas que retiren el equipo y el software extranjeros para 2022 (YANG; LIU, 2019). La medida forma parte de una campaña para reducir la dependencia de China de las tecnologías extranjeras, es probable que desacople las cadenas de suministro entre EE. UU. y China y podría dar un golpe significativo a las empresas estadounidenses (YANG; LIU, 2019). Las nuevas sanciones impuestas añadieron urgencia al proyecto. A diferencia de los esfuerzos anteriores de autosuficiencia tecnológica, el objetivo es que las empresas y el gobierno pronto estén libres de amenazas (YANG; LIU, 2019).

Sin embargo, reemplazar el hardware y el software de EE. UU. con equivalentes chinos también plantea problemas. Lenovo de China utiliza procesadores fabricados por Intel y discos duros fabricados por Samsung de Corea del Sur (YANG; LIU, 2019). China va a la zaga de EE. UU. en algunas de las tecnologías más avanzadas, incluido el diseño y la fabricación de chips. Intel y Qualcomm fabrican componentes clave para algunas de las empresas tecnológicas más grandes del país. El sistema operativo más utilizado en dispositivos fabricados en China es Google Android en teléfonos inteligentes y tabletas o Microsoft Windows en computadoras (SHIDONG, 2019).

En 2019, EE. UU. subió el tono con la Orden Ejecutiva sobre la Seguridad de la Cadena de Suministro de Tecnologías y Servicios de la Información y Comunicación, que establece:

> La adquisición o el uso sin restricciones en los Estados Unidos de tecnología de información y comunicación o servicios diseñados, desarrollados, fabricados o proporcionados por personas de propiedad, controladas o sujetas a la jurisdicción o dirección de adversarios extranjeros aumenta la capacidad de los adversarios extranjeros para crear y explotar vulnerabilidades en tecnología o servicios de información y comunicación, con efectos potencialmente catastróficos y, por lo tanto, representando una amenaza inusual y extraordinaria para la seguridad nacional, la política exterior y la economía de los Estados Unidos (TRUMP, 2019, n.p.).

Luego, en 2020, la confrontación entre EE. UU. y China ganó un nuevo capítulo, que involucró a la aplicación TikTok, utilizada para publicar videos cortos, controlados por la empresa china ByteDance, que supuestamente representan amenazas para la Seguridad Nacional. Todavía no está claro cuáles serían estas amenazas, pero es importante tener en cuenta que la información relevante para la Seguridad Nacional se puede obtener de fuentes insospechadas. En 2018, los datos de una inofensiva aplicación de seguimiento del estado físico llamada Strava revelaron la ubicación de las bases secretas del Ejército de los EE. UU. en todo el mundo. La compañía lanzó mapas que identifican "rutas de carreras populares en las principales ciudades o identifican a personas en áreas más remotas que tienen patrones de ejercicio inusuales". No obstante, "los analistas militares han notado que el mapa también es lo suficientemente detallado como para proporcionar información extremadamente confidencial sobre un subconjunto de usuarios de Strava: militares en servicio activo" (HERN, 2020).

Cualquiera que sea la razón, en el caso de Tik Tok, el gobierno de EE. UU. tenía la intención de forzar la venta de su operación local a una empresa estadounidense. El apoyo legal es proporcionado por el Comité de Inversión Extranjera en los Estados Unidos (CFIUS) bajo la Ley de Producción de Defensa de 1950 (UNITED STATES, [2022b]). CFIUS puede bloquear la adquisición de empresas estadounidenses por parte de inversores extranjeros. En 2018, ByteDance compró TikTok, entonces llamada Music.ly, también una empresa china. Pero Music.ly, a pesar de ser chino, según las regulaciones de CFIUS, se considera "negocio estadounidense", como una entidad que se dedica al comercio interestatal en los Estados Unidos. Por lo tanto, CFIUS puede forzar la operación de EE. UU. a una empresa de propiedad estadounidense, ya que ByteDance no buscó la aprobación de CFIUS en el momento de la adquisición (CHESNEY, 2020).

7 Conlusión

Este artículo buscó demostrar cómo el Ciberespacio, la Logística y la Seguridad Nacional representan serias amenazas entre sí. No necesariamente en el orden habitual de causalidad perceptible, sino en cualquier orden elegido. Un conjunto prolífico de decenas de casos, en su mayoría relacionados con potencias cibernéticas como Estados Unidos y China, bien como el Reino Unido, Alemania y gobiernos y empresas privadas de otras naciones, han proporcionado pruebas empíricas sólidas para respaldar este argumento.

En primer lugar, se mostró cómo la búsqueda de una mejor logística conduce a un aumento de la automatización y, por tanto, a un mayor soporte logístico informatizado. Esta creciente automatización, junto con el uso cada vez mayor de comunicaciones digitales, vehículos autónomos, inteligencia artificial y fabricación aditiva (impresión 3D), entre otras nuevas tecnologías, plantea riesgos crecientes de explotar las vulnerabilidades cibernéticas y permitir la paralización logística de las fuerzas y sociedades militares. Presentando así muchas oportunidades para comprometer la Seguridad Nacional. Desde 2018, ha habido un aumento en el ritmo de las medidas tomadas (o iniciadas) por los gobiernos de las potencias cibernéticas para reducir este riesgo. Sin embargo, como argumenta este artículo, se trataba de una percepción clásica y más de sentido común.

En segundo lugar, mucho menos evidente que el primero, el artículo mostró cómo la logística cada vez más compleja plantea riesgos para la confiabilidad y el desempeño de los productos de hardware y software. Como se muestra, al igual que un componente electromecánico sintonizado infiltrado en cualquier parte de la extensa cadena de suministro de equipos militares, software o los componentes de hardware alterados malintencionadamente pueden comprometer su confiabilidad o rendimiento. Por tanto, también afecta a la Seguridad Nacional. Para ello, se presentó el concepto de cadenas de suministro cibernéticas, y cómo su complejidad trasciende las fronteras nacionales, exigiendo mucha investigación e inversiones para crear y mantener controles que incrementen la seguridad de estos productos, siendo lo suficientemente fluidos como para no volverse muy rígido y lento su desarrollo. Un hecho concreto que dificulta este control es que la cadena de producción de hardware y software es altamente compleja,

con muchos puntos de contacto distribuidos en diferentes partes del mundo. Por ejemplo, las computadoras fabricadas en Brasil pueden tener simultáneamente circuitos y chips diseñados en EE. UU., Alemania y Japón, y producidos en China, Taiwán, Singapur, Vietnam e India, cuyo firmware se produjo en muchos otros países. Asimismo, los grandes y complejos sistemas de software modernos también se construyen en centros de desarrollo repartidos en varios países por técnicos de otros países.

En tercer lugar, también se demostró cómo las decisiones basadas en Seguridad Nacional, como la restricción de la exportación (o importación) de componentes de TI hacia o desde países extranjeros, pueden comprometer las cadenas de suministro de hardware y software (logística) y el ritmo de desarrollo del ciberespacio. No solo en las naciones que son sus principales objetivos, sino también en aquellas que implementan estas medidas. Como se explicó, reemplazar los componentes suministrados en el extranjero con componentes autóctonos (o de terceros "neutrales"), si no es una tarea hercúlea como el control de la cadena de suministro cibernética, también es un esfuerzo costoso y que requiere tiempo.

En general, el artículo muestra que la percepción ha evolucionado desde una amenaza estática, cerrada dentro del perímetro de la nación, el gobierno o la producción de defensa, a un peligro dinámico presente en toda la cadena de suministro, en particular los proveedores privados.

La mala noticia es que proteger las tres áreas es una tarea muy compleja. Además, su viabilidad aún requiere mucha investigación, especialmente en lo que respecta a los activos de alta tecnología de la Base Industrial de Defensa, las empresas que brindan a los gobiernos productos y servicios relacionados con la Seguridad Nacional.

La buena noticia es que ya se han hecho grandes esfuerzos en el tema a nivel internacional, con abundante material disponible, lo que nos permite ahorrar tiempo y recursos para implementar diversas prácticas adoptadas por la industria de clase mundial. Más importante aún, existe una creciente comprensión de que el tema debe abordarse de acuerdo con su relevancia.

Por ahora, la única certeza es que las cadenas de suministro globales relacionadas con el ciberespacio y la Seguridad Nacional estarán bajo un escrutinio mucho mayor que en la actualidad. Además, se puede esperar un enfoque nacionalista considerablemente mayor, que posiblemente (o probablemente) cambie profundamente lo que se ha considerado el núcleo de la tendencia reciente hacia la globalización.

Agradecimientos

El autor agradece a los revisores que contribuyeron al perfeccionamiento de este trabajo.

Referencias

ADAMS, James. Virtual defense. **Foreign Affairs**, [New York], v. 80, n. 3, p. 98, May/June 2001.

ALLEVEN, Monica. Deutsche Telekom selects Ericsson for 5G RAN in Germany. **FierceWireless**, [*s. l.*], July 22, 2020. Disponible en: https://www.fiercewireless.com/operators/deutsche-telekom-selects-ericsson-for-5g-ran-germany. Accesado el: Julio 28, 2022.

AMADO, Guilherme *et al.* O recado das Forças Armadas ao Ministério da Defesa sobre o 5G. *Época*, 7 ago. 2020. Disponible en: https://epoca.globo.com/guilherme-amado/o-recado-das-forcas-armadas-ao-ministerio-da-defesa-sobre-5g-24571588. Accesado el: Julio 28, 2022.

ARON, Raymond. **Paz e guerra entre as nações**. São Paulo: Imprensa Oficial do Estado, 2002.

AUCHARD, Eric; FINKLE, Jim. Ukraine utility cyber attack wider than reported. **Reuters**, [Eagan], Jan. 3, 2016. Disponible en: http://www.reuters.com/article/us-ukraine-crisis-malware-idUSKBN0UI23S20160104. Accesado el: Julio 28, 2022.

BEAUFRE, André. **Introduction to strategy**. London: Faber and Faber Limited, 1965.

BIDEN JR, Joseph R. Executive Order on America's Supply Chains. *In*: THE WHITE HOUSE. Washington, DC: The White House, Feb. 24, 2022. Disponible en: https://www.whitehouse.gov/briefing-room/presidential-actions/2021/02/24/executive-order-on-americas-supply-chains/. Accesado el: Ago. 1, 2022.

BLESSMAN, Danika. Protecting your software supply chain. **Risk Management**, [*s. l.*], n. 1, p. 10-11, 2019.

BLUMENTHAL, Eli. 'Unfixable' hole in Intel ROM exposes all but latest chips to attack, researchers say. **CNet**, [*s. l.*], Mar. 6, 2020. Disponible en: https://www.cnet.com/news/unfixable-hole-in-intel-rom-exposes-all-but-latest-chips-to-attack/. Accesado el: Ago. 3, 2022.

BRYAN, Joseph M. *et al.* **Inquiry into cyber intrusions affecting U.S. Transportation Command contractors**. Washington: U.S. Senate, 2014. Disponible en: https://www.armed-services.senate.gov/imo/media/doc/SASC_Cyberreport_091714.pdf. Accesado el: Ago. 3, 2022.

BURTON, Phillip; MCBIRNEY, Samantha. Military yet to fully leverage additive manufacturing. **National Defense**, Arlington, VA, Feb. 16, 2022. Disponible en: https://www.nationaldefensemagazine.org/articles/2022/2/16/military-yet-to-fully-leverage-additive-manufacturing. Accesado el: Ago. 3, 2022.

CHESNEY, Robert. TikTok and the law: a primer (in case you need to explain things to your teenager). **Lawfare**, [*s. l.*], Ago. 2, 2020. Disponible en: https://www.lawfareblog.com/tiktok-and-law-primer-case-you-need-explain-things-your-teenager. Accesado el: Ago. 3, 2022.

CIMPANU, Catalin. Cisco removed its seventh backdoor account this year, and that's a good thing. **ZDNet**, [*s. l.*], Nov. 7, 2018. Disponible en: https://www.zdnet.com/article/cisco-removed-its-seventh-backdoor-account-this-year-and-thats-a-good-thing/. Accesado el: Ago. 3, 2022.

CISCO. **Cisco prime home authentication bypass vulnerability**. San Jose, CA: Cisco, Feb. 2017. Disponible en: https://www.cisco.com/c/en/us/support/docs/csa/cisco-sa-20170201-prime-home.html. Accesado el: Ago. 3, 2022.

CLARK, Don. U.S. Agencies block technology exports for supercomputer in China. **The Wall Street Journal**, New York, Apr. 9, 2015. Disponible en: https://www.wsj.com/articles/u-s-agencies-block-technology-exports-for-supercomputer-in-china-1428561987. Accesado el: Ago. 3, 2022.

CLAUSEWITZ, Carl Von. **On war**. Princeton: Princeton University Press, 1976.

CORERA, Gordon. US warns of supply chain cyber-attacks. **BBC**, London, Julio 26, 2018. Disponible en: http://bbc.co.uk/news/technology-44941875. Accesado el: Ago. 3, 2022.

EPSHTEIN, Uriel; FAINT, Charles. That's logistics: the autonomous future of the Army's Battlefield. *In*: MODERN WAR INSTITUTE. West Point, NY: Modern War Institute, Jan. 2019. Disponible en: https://mwi.usma.edu/thats-logistics-autonomous-future-armys-battlefield-supply-chain/. Accesado el: Ago. 3, 2022.

ERICSSON. Press Releases. **Deutsche Telekom and Ericsson strengthen partnership with 5G deal**. Stockholm: Ericsson, 2020. Disponible en: https://www.ericsson.com/en/press-releases/2020/7/deutsche-telekom-and-ericsson-strengthen-partnership-with-5g-deal. Accesado el: Ago. 3, 2022.

FREEDMAN, Lawrence. **Strategic coercion**: concepts and cases. Oxford: Oxford University Press, 1998.

FREEDMAN, Lawrence. **Strategy**: a history. Oxford: Oxford University Press, 2015.

GERRING, John. Mere description. **British Journal of Political Science**, [London], v. 42, p. 721-746, 2012. Disponible en: https://cupdf.com/document/gerring-j-mere-description.html?page=1. Accesado el: Ago. 3, 2022.

GOODIN, Dan. Cisco confirms NSA-linked zeroday targeted its firewalls for years. **Ars Tchnica**, [California], Ago. 17, 2016. Disponible en: https://arstechnica.com/security/2016/08/cisco-confirms-nsa-linked-zeroday-targeted-its-firewalls-for-years/. Accesado el: Ago. 3, 2022.

GRAY, Colin. Why strategy is dificult? *In*: MAHNKEN, T. G.; MAIOLO, J. A. (org.). **Strategic studies**. Oxon: Routledge, 2008. p. 40-47.

GREENWALD, Glenn. **No place to hide**: Edward Snowden, the NSA and the surveillance state. [london]: Penguin Books, 2014.

HALFHILL, Tom R. The truth behind the Pentium Bug. **Byte**, California, Mar. 1995. Disponible en: https://web.archive.org/web/20060209005434/http://www.byte.com/art/9503/sec13/art1.htm. Accesado el: Ago. 3, 2022.

HERN, Alex. Oracle in talks with TikTok that could hijack Microsoft bid. **The Guardian**, London, Ago. 2020. Disponible en: https://www.theguardian.com/technology/2020/aug/18/software-firm-oracle-in-talks-to-buy-tiktok-and-challenge-microsoft-bid. Accesado el: Ago. 3, 2022.

HOWARD, Michael. The forgotten dimensions of strategy. **Foreign Affairs**, [New York], v. 57, n. 5, p. 975, 1979.

HUTCHINS, Eric M.; AMIN, Rohan M; CLOPPERT, Michael J. **Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains**. [*S. l.*: *s. n*.], 2010. Disponible en: https://community.mis.temple.edu/mis5208sp2016/files/2015/01/iciw2011.pdf. Accesado el: Ago. 3, 2022.

JAGODA, Jeneé *et al.* The viability and simplicity of 3D-Printed construction: a military case study. **Infrastructures**, [*s. l.*], v. 5, n. 4, p. 1-10, 2020.

JOMINI, Antoine. **The art of war**. 3. ed. Rockville: Arc Manor, 1862.

KHARPAL, Arjun. US should take stake in Nokia, Ericsson to counter Huawei in 5G: Barr. **CNBC**, [Englewood Cliffs, NJ], 2020.

KRESS, Moshe. **Operational logistics**: the art and science of sustaining military operations. New York: Springer Science+Business Media, 2002.

LEE, Micah; MOLTKE, Henrik. Everybody does it: the messy truth about infiltrating computer supply chains. **The Intercept**, [New York], Jan. 24, 2019. Disponible en: https://theintercept.com/2019/01/24/computer-supply-chain-attacks/. Accesado el: Ago. 3, 2022.

LEWIS, James. **Technological competition and China**. Washington, DC: Center for Strategic & International Studies, Nov. 2018. Disponible en: https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/181130_Technological_Competition_and_China.pdf. Accesado el: Ago. 3, 2022.

LIDDELL HART, Basil. Economic pressure or continental victories. **Royal United Services Institution Journal**, [London], v. 76, n. 503, p. 486-510, 1931.

LIDDELL HART, Basil. The essence of war. **Royal United Services Institution Journal**, [London], v. 75, n. 499, p. 490-491, 1930.

LIFF, Adam. Cyberwar: a new "Absolute Weapon"? The proliferation of cyberwarfare capabilities and interstate war. **Journal of Strategic Studies**, London, v. 35, n. 3, p. 401-428, 2012. Disponible en: https://indianstrategicknowledgeonline.com/web/Proliferation%20of%20Cyberwarfare%20Capabilities%20and%20Interstate%20War.pdf. Accesado el: Ago. 3, 2022.

LEIGHTON, Richard. Logistics: military. *In*: ENCYCLOPAEDIA BRITANNICA. [London]: Encyclopaedia Britannica, 2022. Disponible en: https://www.britannica.com/topic/logistics-military. Accesado el: Ago. 3, 2022.

LYNN III, William. Defending a New Domain: the Pentagon's cyberstrategy. **Foreign Affairs**, [New York], v. 89, n. 5, 2010. Disponible en: https://www.foreignaffairs.com/articles/united-states/2010-09-01/defending-new-domain. Accesado el: Ago. 3, 2022.

MICROSOFT. Azure. Resources. **What is Middleware?** [Washington, DC]: Microsoft, 2022. Disponible en: https://azure.microsoft.com/en-us/overview/what-is-middleware/. Accesado el: Ago. 3, 2022.

MILLER, Greg. How the CIA used Crypto AG encryption devices to spy on countries for decades. **The Washington Post**, Washington, DC, 2020.

MOON, Angela. Exclusive: Google suspends some business with Huawei after Trump blacklist - source. **Reuters**, [Eagan], May 19, 2019. Disponible en: https://www.reuters.com/article/us-huawei-tech-alphabet-exclusive/exclusive-google-suspends-some-business-with-huawei-after-trump-blacklist-source-idUKKCN1SP0NB. Accesado el: Ago. 3, 2022.

MORGAN, Patrick. Applicability of traditional deterrence concepts and theory to the cyber realm. *In*: NATIONAL RESEARCH COUNCIL (U.S.). **Proceedings of a workshop on deterring cyberattacks**: informin strategies and developing options for U.S. policy. Washington, DC: National Academies Press, 2010. p. 55-76.

NIST. **Framework for improving critical infrastructure cybersecurity**. [*S. l.*: *s. n.*], 2014. Disponible en: papers2://publication/uuid/DD40979D-D391-4678-9601-F14CF1CB8BF5. Accesado el: Ago. 3, 2022.

NIST; FIREEYE. **Best Practices in Cyber Supply Chain Risk Management**. [California]: National Institute of Standards and Technology, 2015. Disponible en: https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-best-practices-in-cyber-supply-chain-risk-management.pdf. Accesado el: Ago. 3, 2022.

NYE JR, Joseph. Deterrence and dissuasion in cyberspace. **International Security**, [*s. l.*], v. 41, n. 3, p. 44-71, 2017.

PECK, Helen. Supply chain vulnerability, risk and resilience. *In*: WATERS, D. (org.). **Global logistics**: new directions in supply chain management. 6th ed. [*S. l.*]: Kogan Page, 2012. p. 192-207.

PETZINGER, Jill. Deutsche Telekom describes potential Huawei ban as "Armageddon" scenario. **MSN**, June 17, 2020. Disponible en: https://www.msn.com/en-gb/money/technology/deutsche-telekom-describes-potential-huawei-ban-as-armageddon-scenario/ar-BB15BxQM. Accesado el: Ago. 8, 2020.

PROENÇA JÚNIOR, Domício; DUARTE, E. E. The concept of logistics derived from clausewitz: all that is required so that the fighting force can be taken as a given. **Journal of Strategic Studies**, [London], v. 28, n. 4, p. 645-677, 2005. Disponible en: https://www.icesi.edu.co/blogs/estrategialogistica122/files/2012/08/the-concept-of-logistic-derived-from-clausewitz.pdf. Accesado el: Ago. 3, 2022.

ROGERS, Chairman Mike Rogers; RUPPERSBERGER, Dutch. **Investigative report on the U.S. National security issues posed by Chinese telecommunications companies Huawei and ZTE**. Washington, DC: U.S. House of Representatives, Oct. 2012. Disponible en: https://republicans-intelligence.house.gov/sites/intelligence.house.gov/files/documents/huawei-zte%20investigative%20report%20(final).pdf. Accesado el: Ago. 3, 2022.

ROSA, Bruno; ANTUNES, Cláudia. Embaixador dos EUA alerta que se Brasil permitir chinesa Huawei no 5G enfrentará "consequências". **O Globo**, Rio de Janeiro, jul. 29, 2020. Disponible en: https://oglobo.globo.com/economia/embaixador-dos-eua-alerta-que-se-brasil-permitir-chinesa-huawei-no-5g-enfrentara-consequencias-24555785. Accesado el: Ago. 3, 2022.

SANGER, David; PERLROTH, Nicole. FBI Confirms DarkSide as Colonial Pipeline Hacker. **The New York Times**, New York, May 10, 2021. Disponible en: https://www.nytimes.com/2021/05/10/us/politics/pipeline-hack-darkside.html. Accesado el: Ago. 3, 2022.

SCHWAAR, Carolyn. U.S. Military To 3D print its way out of supply chain woes. **Forbes**, Feb. 27, 2022. Disponible en: https://www.scmp.com/business/article/3011377/china-offers-five-year-tax-breaks-chip-makers-software-developers-bolster https://www.forbes.com/sites/carolynschwaar/2022/02/27/us-military-to-3d-print-its-way-out-of-supply-chain-woes/?sh=316b8598275d. Accesado el: Ago. 4, 2022.

SHERMAN, Mark. **Growing risks in the software supply chain**: Platform Security Summit 2019. [*S. l.*]: Software Engineering Institute; Carnegie Mellon Univerty, Oct. 2019. Disponible en: https://www.platformsecuritysummit.com/2019/speaker/sherman/PSEC2019-Risks-Software-Supply-Chain-Mark-Sherman.pdf. Accesado el: Ago. 4, 2022.

SHIDONG, Zhang. China offers five-year tax breaks to chip makers, software developers to bolster industry as trade war stretches to tech. **South China Morning Post**, Shanghai, May 22, 2019. Disponible en: https://www.scmp.com/business/article/3011377/china-offers-five-year-tax-breaks-chip-makers-software-developers-bolster. Accesado el: Ago. 2, 2022.

STONE, John. Technology and war: a trinitarian analysis. **Defense & Security Analysis**, [London], v. 23, n. 1, p. 27-40, 2007.

STRUMPF, Dan. Huawei's 5G dominance threatened by U.S. Policy on Chips. **The Wall Street Journal**, New York, 2020. Disponible en: https://www.wsj.com/articles/huawei-struggles-to-escape-u-s-grasp-on-chips-11592740800. Accesado el: Ago. 2, 2022.

SUPPLY chains are undergoing a dramatic transformation. **The Economist**, New York, p. 1-7, July 11, 2019. Disponible en: https://www.economist.com/special-report/2019/07/11/supply-chains-are-undergoing-a-dramatic-transformation. Accesado el: Ago. 2, 2022.

TOP500.ORG. Lists. **Top500 June 2020**. Sinsheim: Top500.org, 2020. Disponible en: https://www.top500.org/lists/top500/2020/06/. Accesado el: Ago. 2, 2022.

TRUMP, Donald J. Executive Order on securing the information and communications technology and services supply chain (EO15873). *In*: THE WHITE HOUSE. Washington, DC: The white House, May 15, 2019. Disponible en: https://trumpwhitehouse.archives.gov/presidential-actions/executive-order-securing-information-communications-technology-services-supply-chain/. Accesado el: Ago. 2, 2022.

TURNBULL, Benjamin. Cyber-resilient Supply chains: mission assurance in the future operating environment. **Australian Army Journal**, [Canberra], v. 14, n. 3, p. 41-56, 2018. Disponible en: https://search.informit.org/doi/pdf/10.3316/informit.344417545553155. Accesado el: Ago. 1, 2022.

TZU, Sun. **The Art of War (Restored Translation)**. [*S. l.*]: Pax Librorum, 2009.

UNITED STATES. Defense Logistics Agency. **Defense Logistics Agency strategic plan 2015-2022**. [Virginia]: Defense Logistics Agency, 2015. Disponible en: https://www.dla.mil/Portals/104/Documents/Headquarters/History/StrategicPlans/2015%20-%202022%20Strategic%20Plan.pdf. Accesado el: July 28, 2022.

UNITED STATES. Department of Commerce. **Announces the addition of Huawei Technologies Co. Ltd. to the entity list**. Washington, DC: U.S. Department of Commerce, 2019. Disponible en: https://www.commerce.gov/news/press-releases/2019/05/department-commerce-announces-addition-huawei-technologies-co-ltd. Accesado el: Ago. 4, 2022.

UNITED STATES. Department of Defense. **Department of Defense Additive Manufacturing Strategy**. Washington, DC: Department of Defense, Jan. 2021a. Disponible en: https://www.cto.mil/wp-content/uploads/2021/01/dod-additive-manufacturing-strategy.pdf. Accesado el: Ago. 4, 2022.

UNITE STATES. Department of Defense and General Services Admnistration. **Improving cybersecurity and resilience through acquisition**: final report of the Department of Defense and General Services Admnistration. [Washington, DC: Department of Defense and General Services Admnistration], Nov. 2013a. Disponible en: https://www.gsa.gov/cdnstatic/IMPROVING_CYBERSECURITY_AND_RESILIENCE_THROUGH_ACQUISITION.pdf. Accesado el: Ago. 3, 2022.

UNITED STATES. Department of Defense. Defense Science Board. **Cyber supply chain**. Washington, DC: Defense Science Board, 2017.

UNITED STATES. Department of Defense. Defense Science Board. **Resilient Military systems and the advanced cyber threat**. Washington, DC: Defense Science Bord, 2013b. (Task force report). Disponible en: https://apps.dtic.mil/sti/pdfs/ADA569975.pdf. Accesado el: Ago. 4, 2022.

UNITED STATES. Department of Defense. **Department of Defense Strategy for Operating in cyberspace**. Washington, DC: Department of Defense, July 2011. Disponible en: https://csrc.nist.gov/CSRC/media/Projects/ISPAB/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf. Accesado el: Ago. 4, 2022.

UNITED STATES. Department of Defense. **DoD Open Source Software (OSS) FAQ**. Washington, DC: Department of Defense, Out. 28, 2021b. Disponible en: https://dodcio.defense.gov/open-source-software-faq/. Accesado el: Ago. 4, 2022.

UNITED STATES. Department of Defense. Securing Defense-Critical Supply Chains: an action plan developed in response to President Biden's Executive Order 14017. Washington, USA: Department of Defense, Feb. 2022a. Disponible en: https://media.defense.gov/2022/Feb/24/2002944158/-1/-1/1/DOD-EO-14017-REPORT-SECURING-DEFENSE-CRITICAL-SUPPLY-CHAINS.PDF. Accesado el: Ago. 4, 2022.

UNITED STATES. Department of Treasury Policy issues. International. **The Committee on Foreign Investment in the United States (CFIUS)**. Washington, DC: US Department of the Treasury, [2022b]. Disponible en: https://home.treasury.gov/policy-issues/international/the-committee-on-foreign-investment-in-the-united-states-cfius. Accesado el: Ago. 2, 2022.

UNITED STATES. **Foreign economic espionage in cyberspace**. [*S. l.*: *s. n.*], 2018.

VEGETIUS, Flavius Renatus. **De Re Militari**. [*S. l.*: *s. n.*], 1767.

WILLETT, Marcus. Lessons of the SolarWinds Hack. **Survival**, [London], v. 63, n. 2, p. 7-26, 2021.

WOOD, Donald F. Logistics: business. *In*: ENCYCLOPAEDIA BRITANNICA. [London]: Encyclopaedia Britannica, 1998. Disponible en: https://www.britannica.com/topic/logistics-business. Accesado el: Ago. 3, 2022.

WOODS, Beau; BOCHMAN, Andy. **Supply chain in the software era**. Washington, DC: Atlantic Council, May 2018. Disponible en: https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/supply-chain-in-the-software-era/. Accesado el: Ago. 1, 2022.

YANG, Yuan; LIU, Nian. Beijing orders state offices to replace foreign PCs and software. **Financial Times**, [London], Dec. 8, 2019. Disponible en: https://www.ft.com/content/b55fc6ee-1787-11ea-8d73-6303645ac406. Accesado el: Ago. 1, 2022.

ZETTER, Kim. **Countdown to Zero Day**: Stuxnet and the Launch of the World's First Digital Weapon. New York: Crown, 2015a.

ZETTER, Kim. Everything we know about Ukraine's Power Plant Hack. **Wired**, Boone, IA, Jan. 28, 2016. Disponible en: https://www.wired.com/2016/01/everything-we-know-about-ukraines-power-plant-hack/. Accesado el: Ago. 1, 2022.

ZETTER, Kim. Suite of sophisticated NationState attack tools found with connection to Stuxnet. **Wired**, boone, IA, Feb 16, 2015b. Disponible en: https://www.wired.com/2015/02/kapersky-discovers-equation-group/. Accesado el: Ago. 1, 2022.


ECEME